[CLAIMS]

1. A method for a base station to manage a traffic encryption key for encrypting traffic data for a multicast service or a broadcast service provided to a subscriber station in a wireless portable Internet system, the method comprising:

(a) generating a new traffic encryption key so as to update a current traffic encryption key when a predetermined time elapses from a start time of an active lifetime of the current traffic encryption key used for encrypting traffic data currently transmitted to the subscriber station; and

(b) transmitting the new traffic encryption key to subscriber stations provided with the multicast service or the broadcast service through a broadcast connection.

2. A method for a base station to manage a traffic encryption key for encrypting traffic data for a multicast service or a broadcast service provided to a subscriber station in a wireless portable Internet system, the method comprising:

(a) generating a specific key for encrypting or decrypting a traffic encryption key before a predetermined time elapses from a start time of an active lifetime of the current traffic encryption key used for encrypting traffic data currently transmitted to the subscriber station;

(b) transmitting the specific key to subscriber stations receiving the multicast service or the broadcast service through a primary management connection;

(c) generating a new traffic encryption key so as to update the current traffic encryption key when the predetermined time elapses from a start time of an active lifetime of the current traffic encryption key; and

(d) transmitting the new traffic encryption key to subscriber stations receiving the multicast service or the broadcast service through a broadcast connection to update a traffic encryption key used by the subscriber station.

3. The method of claim 1 or 2, wherein the predetermined time is established to be a time which is prior to an expiration time of an active lifetime of the current traffic encryption key by a multicast & broadcast (M&B) TEK Grace Time based on the M&B TEK Grace Time managed by the base station.

4. The method of claim 1, wherein in (b), a Key Reply message included in a Privacy Key Management Response (PKM-RSP) message of the IEEE 802.16 is used to transmit the new traffic encryption key to the subscriber station through the broadcast connection.

5. The method of claim 1, wherein in (a), the new traffic encryption key is encrypted by the current traffic encryption key through the 3-Data Encryption Standard (3-DES) or Advanced Encryption Standard (AES).

6. The method of claim 1, wherein the method further comprises, before (a):

(i) receiving a request on a traffic encryption key for a multicast

service or a broadcast service from the subscriber station so as to initially receive the multicast service or the broadcast service; and

(ii) generating a requested traffic encryption key and transmitting the generated traffic encryption key to the subscriber station,

wherein message transmission between the base station and the subscriber station is performed through a Primary Management Connection of the IEEE 802.16.

7. The method of claim 6, wherein the traffic encryption key generated in (ii) is encrypted using the 3-Data Encryption Standard (3-DES) or Advanced Encryption Standard (AES), and is encrypted by a Key Encryption Key (KEK) generated by an Authentication Key (AK) of the subscriber station.

8. The method of claim 1, wherein in (b), an active lifetime of the new traffic encryption key starts when the new traffic encryption key is transmitted to the subscriber station to update the current traffic encryption key and the active lifetime of the current traffic encryption key expires.

9. The method of claim 2, wherein in (b), the specific key is a Group Key Encryption Key (GKEK) distributed to the subscriber stations served with the multicast service or the broadcast service.

10. The method of claim 9, wherein the GKEK is encrypted by the Authorization Key (AK) of the subscriber station served with the multicast service or the broadcast service.

11. The method of claim 2, wherein the method further comprises, before (a):

(i) receiving a request on a traffic encryption key for a multicast service or a broadcast service from the subscriber station so as to initially receive the multicast service or the broadcast service; and

(ii) generating a requested traffic encryption key and transmitting the generated traffic encryption key to the subscriber station,

wherein message transmission between the base station and the subscriber station is performed through a Primary Management Connection of the IEEE 802.16.

12. The method of claim 11, wherein a Key Reply message included in a privacy Key Management Response (PKM-RSP) message of the IEEE 802.16 is used to transmit the generated traffic encryption key in (ii) to the subscriber station, and the Key Reply message includes the specific key for encrypting the traffic encryption key.

13. The method of any one of claims 9, 10, and 12, wherein the GKEK managed for each multicast service or the broadcast service is randomly generated by the base station or an Authentication Authorization and Accounting (AAA) server for accessing the base station and authenticating the subscriber.

14. The method of claim 13, wherein the base station randomly generates the GKEK when the range of the multicast service or the broadcast service covers a base station.

15. The method of claim 13, wherein the AAA server randomly generates the GKEK when the range of the multicast service or the broadcast service covers the wireless portable Internet system.

16. The method of claim 2, wherein in (c), the new traffic encryption key is encrypted through the 3-Data Encryption Standard (3-DES) or Advanced Encryption Standard (AES), and is encrypted by a specific key transmitted to the subscriber station in (b).

17. The method of claim 2, wherein in (d), an active lifetime of the new traffic encryption key starts when the new traffic encryption key is transmitted to the subscriber station to update the current traffic encryption key and the active lifetime of the current traffic encryption key expires.

18. The method of claim 1 or 2, wherein the base station transmits the current traffic encryption key and the new traffic encryption key to the subscriber stations having initially requested the traffic encryption key, when receiving the request on the traffic encryption key from the subscriber station after the predetermined time elapses from the start time of the active lifetime of the current traffic encryption key.

19. The method of claim 1 or 2, wherein the base station transmits the new traffic encryption key to the subscriber stations having requested the traffic encryption key, when receiving a request on the traffic encryption key from the subscriber station so as to update the current traffic encryption key while the subscriber station receives the

multicast service or the broadcast service after the predetermined time elapses from the start time of the active lifetime of the current traffic encryption key.

20. The method of claim 18 or 19, wherein the traffic encryption key request and transmission generated after the predetermined time is performed by each base station and subscriber station through the Primary Management Connection.

21. A method for a subscriber station to manage a traffic encryption key for decrypting traffic data for a multicast service or a broadcast service received from a base station in a wireless portable Internet system, the method comprising:

(a) receiving a new traffic encryption key from the base station through a broadcast connection; and

(b) updating a current traffic encryption key with the new traffic encryption key, and using the new traffic encryption key to decrypt traffic data received from the base station.

22. A method for a subscriber station to manage a traffic encryption key for decrypting traffic data for a multicast service or a broadcast service received from a base station in a wireless portable Internet system, the method comprising:

(a) receiving a new specific key for decrypting a traffic encryption key from the base station through a Primary Management Connection, the new specific key being encrypted with an Authorization Key (AK) allocated

when the subscriber station is authenticated;

(b) updating a current specific key with the new specific key;

(c) receiving a new traffic encryption key from the base station through a broadcast connection, the new traffic encryption key being encrypted with the new specific key; and

(d) decrypting the new traffic encryption key with the new specific key to update the current traffic encryption key, and using the updated traffic encryption key to decrypt traffic data received from the base station.

23. The method of claim 21, wherein the subscriber station receives the new traffic encryption key from the base station after a first specific time elapses from a start time of an active lifetime of the current traffic encryption key.

24. The method of claim 22, wherein the subscriber station receives the new specific key from the base station before a first specific time elapses from a start time of an active lifetime of the current traffic encryption key, and receives the new traffic encryption key therefrom after the first specific time elapses from the start time thereof.

25. The method of claim 23 or 24, wherein the first specific time is established to be a time which is prior to an expiration time of an active lifetime of the current traffic encryption key by a multicast & broadcast (M&B) TEK Grace Time based on the M&B TEK Grace Time managed by the base station.

26. The method of claim 25, wherein the subscriber station

requests no traffic encryption key update when receiving a new traffic encryption key from the base station through the broadcast connection before a second specific time elapses.

27. The method of claim 26, wherein the second specific time is established based on a TEK Grace Time managed by the subscriber station, and is established to be a time which is prior to an expiration time of the active lifetime of the current traffic encryption key by the TEK Grace Time.

28. The method of claim 27, wherein the M&B TEK Grace Time is established to be greater than the TEK Grace Time.

29. The method of claim 23 or 24, wherein an active lifetime of the new traffic encryption key starts when the active lifetime of the current traffic encryption key expires after the current traffic encryption key is updated with the new traffic encryption key.

30. The method of claim 25, wherein the method comprises:

when the subscriber station receives no new traffic encryption key from the base station through the broadcast connection until the second specific time expires,

requesting a new traffic encryption key from the base station through a Primary Management Connection and receiving the new traffic encryption key so as to update the current traffic encryption key; and

updating the current traffic encryption key with the new traffic encryption key, and using the new traffic encryption key to decrypt traffic

data received from the base station.

31. A method for configuring a protocol for managing a traffic encryption key for encryption or decryption of traffic data for a multicast service or a broadcast service transmitted and received between a subscriber station and a base station in a wireless portable Internet system, the method comprising:

(a) the subscriber station using a MAC message to transmit a Key Request message to the base station and request a traffic encryption key;

(b) the base station using the MAC message to transmit a Key Reply message including the requested new traffic encryption key and a specific key to the subscriber station, the specific key being encrypted with an Authorization Key allocated to the subscriber station and being used to encrypt the traffic encryption key;

(c) the base station using the MAC message to transmit the first Key Update Command message including a new specific key to the subscriber station so as to update the specific key; and

(d) the base station using the MAC message to transmit the second Key Update Command message including a new traffic encryption key encrypted by the new specific key to the subscriber station.

32. The method of claim 31, wherein in (a), the subscriber station transmits the Key Request message included in a Privacy Key Management Request (PKM-REQ) message of the IEEE 802.16 to the base station through a Primary Management Connection.

33. The method of claim 31, wherein in (b), the subscriber station transmits the Key Reply message included in a Privacy Key Management Response (PKM-RSP) message of the IEEE 802.16 to the base station through a Primary Management Connection.

34. The method of claim 33, wherein the specific key includes a Group Key Encryption Key (GKEK) distributed to the subscriber stations served with the multicast service or the broadcast service, and is included in TEK-parameters included in the Key Reply message.

35. The method of claim 31, wherein in (c) and (d), the first Key Update Command message is transmitted through a Primary Management Connection,

the second Key Update Command message is transmitted through a broadcast connection, and

the first Key Update Command message and the second Key Update Command message include: a Key-Sequence-Number parameter; a security association identification (SA-ID) parameter; a Key Push Modes parameter for identifying the first and second Key Update Command messages; a Key Push Counter for preventing replay attacks on the Key Update Command message; TEK-parameters relevant to the traffic encryption key; and an HMAC-Digest for authenticating the first and second Key Update Command messages.

36. The method of claim 35, wherein the TEK-parameters included in the first Key Update Command message include the GKEK

and a traffic encryption key sequence number.

37. The method of claim 35, wherein the TEK-parameters included in the second Key Update Command message include a new traffic encryption key, a Key-Lifetime of the new traffic encryption key, a Key-Sequence-Number, and a Cipher Block Chaining Initialization Vector (CBC-IV) for functioning as an input key for encrypting traffic data.

38. The method of claim 35, wherein when an HMAC authentication key needed as an input key for generating the HMAC-Digest is generated for a downlink;

the Secure Hash Algorithm (SHA) is used to generate the HMAC authentication key;

a downlink HMAC_PAD_D and a Key Push Counter are used as input keys in the first and second Key Update Command messages; and

an authentication key allocated for each subscriber station is used as another input key for the first Key Update Command message authentication, and a GKEK transmitted through the first Key Update Command message is used as another input key for the second Key Update Command message authentication.

39. An operation method of a traffic encryption key state machine provided to a subscriber station and used for the subscriber station to manage a traffic encryption key for decrypting traffic data received from a base station for a multicast service or a broadcast service, the operation method comprising:

transmitting a Key Request message to the base station according to generation of a traffic encryption key request event and then entering an Op Wait state; and

controlling an Operational state being able to receive the traffic data from the base station,

wherein the traffic encryption key state machine goes to the Operational state and starts a predetermined operation when the subscriber station in an Op Wait state receives a Key Reply message including a new traffic encryption key from the base station.

40. The operation method of claim 39, wherein the method further comprises: using a new traffic encryption key generated and transmitted by the base station according to a request of the subscriber station, and waiting for a re-key (a Re-key Wait state),

wherein the subscriber station transmits a Key Request message to the base station according to a generation of a TEK Refresh Timeout event and the traffic encryption key state machine goes to the Re-key Wait state when the subscriber station fails to receive the Key Reply message for distribution of the new traffic encryption key from the base station in the Operational state.

41. The operation method of claim 40, wherein the traffic encryption key state machine receives the Key Reply message including the new traffic encryption key from the subscriber station in response to the Key Request message by the base station in the Re-key Wait state,

and goes to the Operational state.

42. An operation method of a traffic encryption key state machine existing in a subscriber station and used for the subscriber station to manage a traffic encryption key for decrypting traffic data received from a base station for a multicast service or a broadcast service, the operation method comprising:

transmitting a Key Request message to the base station according to generation of a traffic encryption key request event and then entering an Op Wait state;

controlling an Operational state to receive the traffic data from the base station; and

controlling a Multicast and Broadcast (M&B) Re-key Interim Wait state to momentarily wait for by using a new traffic encryption key automatically generated and transmitted by the base station,

wherein the traffic encryption key state machine goes to the Operational state and starts a predetermined operation when a Key Reply message event is provided from the base station in the Op Wait state,

a GKEK Updated event is generated and the traffic encryption key state machine goes to the M&B Re-key Interim Wait state when a new specific key is provided from the base station through the first Key Update Command message in the Operational state so as to update the specific key, and

a TEK Updated event is generated and the traffic encryption key

state machine goes to the Operational state when the second Key Update Command message for distributing a new traffic encryption key encrypted with the new specific key is transmitted from the base station through a broadcast connection in the M&B Re-key Interim Wait state.

43. The operation method of claim 42, wherein the method further comprises using the new traffic encryption key generated and transmitted by the base station according to a request by the subscriber station, and waiting for a re-key (a Re-key Wait state),

wherein the subscriber station transmits a Key Request message to the base station because of generation of a TEK Refresh Timeout event and the traffic encryption key state machine goes to the Re-key Wait state when failing to receive the first Key Update Command message from the base station and generating no GKEK Updated event in the Operational state.

44. The operation method of claim 43, wherein the subscriber station transmits a Key Request message to the base station because of a generation of a TEK Refresh Timeout event by the subscriber station and the traffic encryption key state machine goes to the Re-key Wait state when failing to receive the second Key Update Command message from the base station and generating no TEK Updated event in the M&B Re-key Interim Wait state.

45. The operation method of claim 43 or 44, wherein the traffic encryption key state machine receives a new traffic encryption key and a

Key Reply message including a new specific key for decrypting the new traffic encryption key from the subscriber station in response to the Key Request message by the base station in the Re-key Wait state, and goes to the Operational state.

5